

TK 155.647

KFKI-1984-68

ZS. SZEGI

COMPUTERIZED OPERATION MANUAL (COM)
OF NUCLEAR POWER PLANTS

Hungarian Academy of Sciences

CENTRAL
RESEARCH
INSTITUTE FOR
PHYSICS

BUDAPEST

COMPUTERIZED OPERATION MANUAL (COM) OF NUCLEAR POWER PLANTS

ZS. SZEGI

Central Research Institute for Physics
H-1525 Budapest 114, P.O.B. 49, Hungary

HU ISSN 0368 5330

ISBN 963 372 255 1

ABSTRACT

This paper is to be presented on International Seminar on Diagnoses of and Response to abnormal occurrences at Nuclear Power Plants organized by the International Atomic Energy Agency. The topic of presentation is the Computerized Operational Manual. This system supports the operator at disturbance situations by displaying quickly and unambiguously the operational instructions and the relevant information without mistakes. By the computerized manual the operator can determine the instruction-subsystem which reflects the real state of the power unit. From this point the system guides the operator how to drive the unit to an other determined state by providing the operational instructions at any time. A data bank is also included which contains information concerning rules restrictions moreover on maintenance and repair. The system will be realized at Paks NPP.

АННОТАЦИЯ

Доклад подготовлен для совещания специалистов МАГАТЭ по теме "Создание и устранение абнормальных режимов АЭС", и содержит методический проект системы Технологических Указаний управления энергоблоком, организованной на ЭВМ. Система с ЭВМ поддерживает оператора блока в абнормальных режимах путем быстрого, однозначного и безошибочного выбора и показа большого количества операций, заложенной в Технологических Указаниях. Система по шагам показывает последовательность операций, с помощью которых состояние энергоблока переведется из одного в другое, и обеспечивает доступ к банку информации АЭС также. Система в каждый момент времени точно показывает актуальное состояние хода исполнения последующих операций. По проектам система Технологических Указаний управления энергоблока будет реализована на втором блоке АЭС Пакш.

KIVONAT

A riport a Nemzetközi Atomenergia Ügynökség által Atomerőművek abnormális működésének diagnózisa és megszüntetése címmel szervezett szemináriumon elhangzó előadás anyagát tartalmazza. Az előadás a számítógépes üzemviteli utasításrendszer metodikai tervét ismerteti, amely az OKKFT A-11 program keretén belül került kidolgozásra. A rendszer az üzemviteli utasítások hatalmas mennyiségének gyors, egyértelmű és hibamentes megjelenítésével segíti az operátort üzemzavari helyzetekben. Lépésről lépésre mutatja az utat, amelyben az erőművi blokkot valamely állapotból egy másik, kívánt állapotba lehet juttatni, s közben információs bank elérését teszi lehetővé. A rendszer minden időpillanatban pontosan tükrözi az utasításának menetét. A számítógépes üzemviteli utasításadó rendszert a Paksi Atomerőműben tervezzük megvalósítani.

Contents

Introduction

1. Functional description
 - 1.1. The operational instruction formats
 - 1.2. The structure of instructions
 - 1.3. How COM supports the operator
2. Information bank
3. The screen-formats
 - 3.1. The operation structure on the screen
 - 3.2. Colouring
4. Storage of operations
 - 4.1. Structure of the storage
 - 4.2. Core
 - 4.3. Libraries
 - 4.4. Saving
5. The Editor function
6. Hardware resource estimation

1. The first part of the report

2. The second part of the report

3. The third part of the report

4. The fourth part of the report

5. The fifth part of the report

6. The sixth part of the report

7. The seventh part of the report

8. The eighth part of the report

9. The ninth part of the report

10. The tenth part of the report

11. The eleventh part of the report

12. The twelfth part of the report

13. The thirteenth part of the report

14. The fourteenth part of the report

15. The fifteenth part of the report

16. The sixteenth part of the report

17. The seventeenth part of the report

18. The eighteenth part of the report

19. The nineteenth part of the report

20. The twentieth part of the report

21. The twenty-first part of the report

22. The twenty-second part of the report

23. The twenty-third part of the report

24. The twenty-fourth part of the report

25. The twenty-fifth part of the report

26. The twenty-sixth part of the report

27. The twenty-seventh part of the report

28. The twenty-eighth part of the report

29. The twenty-ninth part of the report

30. The thirtieth part of the report

31. The thirty-first part of the report

32. The thirty-second part of the report

33. The thirty-third part of the report

34. The thirty-fourth part of the report

35. The thirty-fifth part of the report

36. The thirty-sixth part of the report

37. The thirty-seventh part of the report

Introduction

As it is wellknown after the TMI accident the causes of disturbances arising in complex systems are basically determined by the interactions of the control staff. That means the human factor is very important in operating systems of large complexity.

According to the post-incident analysis of real plant disturbances [1] the main problem was not to realize the disturbance situation but fulfilling the proper procedure. In accident circumstances the operator carried out an improper intervention not corresponding to the Operation Manual of the power unit, so the operator himself changed the developing disturbance to an accident.

The main reasons of that are:

- the stress effect of the accident situation, and
- the operators are not accustomed to rare conditions.

The number of accidents may be decreased on two ways:

- the operators' repeated training by simulators
- fast displaying the operational instructions without mistakes.

These two methods mutually complement each other. The realisation of the Computerized Operation Manual seems to be not quite complicated project but its effect is considerable.

On this topic there are researches and results in some countries [2,3,4,5,6,7,8] .

In Hungary the Computerized Disturbance Analysis and Operator Advisory System of Paks NPP is under development. A part of this work the plan of the Computerized Operation Manual system /COM/ has finished.

1. Functional description

1.1. The operational instruction formats

The basis of the Computerized Manual is the hierarchical structure of instructions arranged into logical and chronological order manually in Paks NPP [9]. In that manual there are three types of instructions:

- conditions
- instructions without condition
- control instructions.

Conditions include description of activity needed to execute if the given situation arises.

The control instructions are themselves executable instructions but their chronological order is determined: they must be carried out after execution of certain instructions. It can be seen that the instructions appearing in the manual can be considered as executable instructions.

According to logical and chronological connections there are three groups of instructions:

- which must be carried out in specified order, that is their time sequence is strictly determined,
- which can be executed in any order - these instructions are in logical AND connection,
- alternative instructions: it is necessary to fulfil at least one of them - or only one of them. That is they are in logical OR connection.

1.2. The structure of instructions

On the highest level of the instruction hierarchy there are the so-called phases. A phase describes a basic activity; the purpose of that is to drive the power unit from a specified state to an other determined state /e.g. start-up,

shut-down/. At a time only one phase is supported by COM.

The following hierarchical level contains the decomposition of phases to operations /e.g. filling a container/. An operation is a well-defined activity of the operator. We suppose that a phase is built as a sequence of operations.

An operation consists of instructions which are located on the lowest levels of the hierarchy. An instruction means an intervention made by the operator. Such an intervention can be active / closing an isolating valve/ or passive /controlling a level measurement/. The instructions are connected to each other by logical operators.

In order to easy handling of large and repeated instruction sequences we had to introduce a further idea: it is the sub-phase. This is an activity sequence which describes a large state change. A sub-phase may occur inside a phase or operation. The structure and form of a sub-phase is the same as the phase.

According to this hierarchical structure the operational instructions may be represented by a tree structure, the nodes of which consist of instructions and Boolean-algebraic relations.

1.3. How COM supports the operator

Starting from the highest level first the operator has to select the basic activity: the phase, then he follows individual subsets of operations or instructions on lower levels.

1.3.1.

At the beginning the list of phases is presented on the display. Later at any time the current phase can be seen in one of the fields of the screen.

1.3.2.

1.3.3.

The system is informed about the fulfilment of an operation instruction or sub-phase by the operator's acknowledgement. The operator has the responsibility for the validity of this acknowledgements.

In a further development phase COM will be connected to the data base of the plant computer which contains information about all of the events happened in the unit during the last periods, thus the COM system will be able to compare the operator's acknowledgements to the real situation. If they will not correspond to each other the system will suspend the operator's further activity until his correction.

In the first development phase the system only guides and helps the operator it sends only warnings if the operator does not follow the instructions, but it does not interrupt the operation.

1.3.4.

The operator is able to announce to COM that he has started the execution of an instruction.

This manipulation mode has importance in the case of instructions being not in time sequence but having long execution time. After starting such an execution others can be also manipulated before finishing the started operation. This kind of parallelism may be applied in the case of AND and OR operations.

1.3.5.

The operator has the possibility to deviate from the manual. If some of the operations cannot be fulfilled in proper way these requirements can be skipped by the operator in order to enable the continuation of the processing, but such decisions must be documented to COM. In the manipulation mode of an instruction, the actual operation is stored in the nodes of the tree structure as the "state" of the instructions. The states on the tree can show the execution way of a phase at every time instant. The states are reflected by satisfactorily chosen colours of the instructions on the screen.

1.3.6.

The operations and sub-phases are mainly complex instructions. It is possible that - due to either the simplicity of the operations or the experience of the operator - someone can fulfil a phase or subphase on the operation level, but in general it is necessary to step onto the lower level of the hierarchy to reach the instruction subsystem. The lower levels deal with the detailed operations and sub-phases which have to be fulfilled. If all instructions of a subset are fulfilled the processing can continue to a further step on higher level.

The manipulation possibilities and modes are the same for the operations and instructions at all levels of the hierarchy.

1.3.7.

During a phase-fulfilment the operator has to manage several hundred activities. Considering the large number of operations the system has to offer a convenient tool for functional search. Direction of the search may be forward and backward. The object of the search may be:

- the first n instructions which were fulfilled or started or skipped;
- the last n instructions, or all instructions of types mentioned above.

2. Information bank

The system will be connected to an information data bank that contains every information concerning rules, restrictions but also for maintenance and repair. The operator must be able to retrieve and display them quickly at every time.

The information bank is an independent data bank but its data base management system can receive references from the COM. In the operation manual a pointer belongs to every instruction which points to that information in the data bank, which would be necessary or useful before the execution.

In the COM system two colour display are planned to provide information separately about the actual operations and on the relevant data stored in the information bank.

The information bank may contain time dependent data which have direct effect to the execution of a process. If the execution time of an operation is limited in the information bank, this requirement must be reported to the operator.

It is important to display the timing pointers with "warning" colour to call operator's attention to the corresponding information in the bank.

In case of time dependent requirements the operator's activity will start a clock and a warning message in warning colour will be displayed with increasing frequency until reaching the time limit.

3. The screen-formats

The main purpose of the system is to provide an effective help to the operator. From this point of view the display formats and colours have great importance. The planned division of the screen into fields and the displayed information can be seen on Figures 2. and 3.

After having chosen the needed phase, the display presents a picture / see Fig.2./ which shows the operation level. If the "subset" field of an operation is not empty, the operator can pass on the lower level of the structure by pressing a specified pushbutton, then the format of detailed operation will be shown on the screen just like in Fig.3.

3.1. The operation structure on the screen

The logical and chronological connection of operations can be displayed by using specified "structure pointing brackets". If we make the following correspondence:

group of instructions being in sequence	↔	[
AND operation	↔	[
OR operation	↔	[

the brackets on Fig.3. denote the structure of Fig.4.

It results from the definition of operations that the brackets may be nested into each other. It must take care to use properly the brackets on the two bounds of the instruction field.

3.2. Colouring

The manipulation mode of the operations will be reflected by colour changes on the screen. The "initial" colour of every operation is kept until the operator informs the system by pressing a specified functional key on the keyboard that he

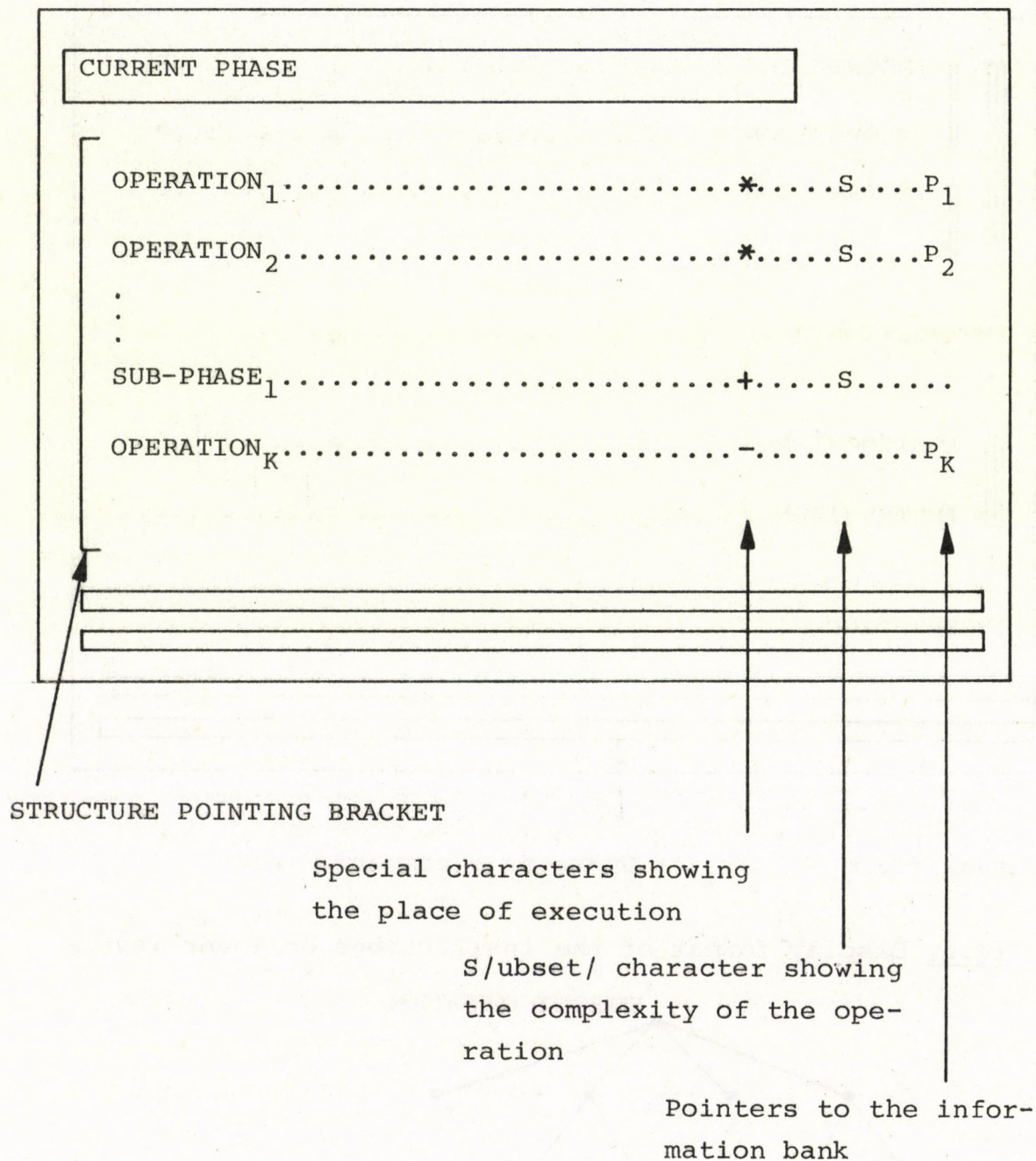


Fig.2. Picture format after choosing the phase

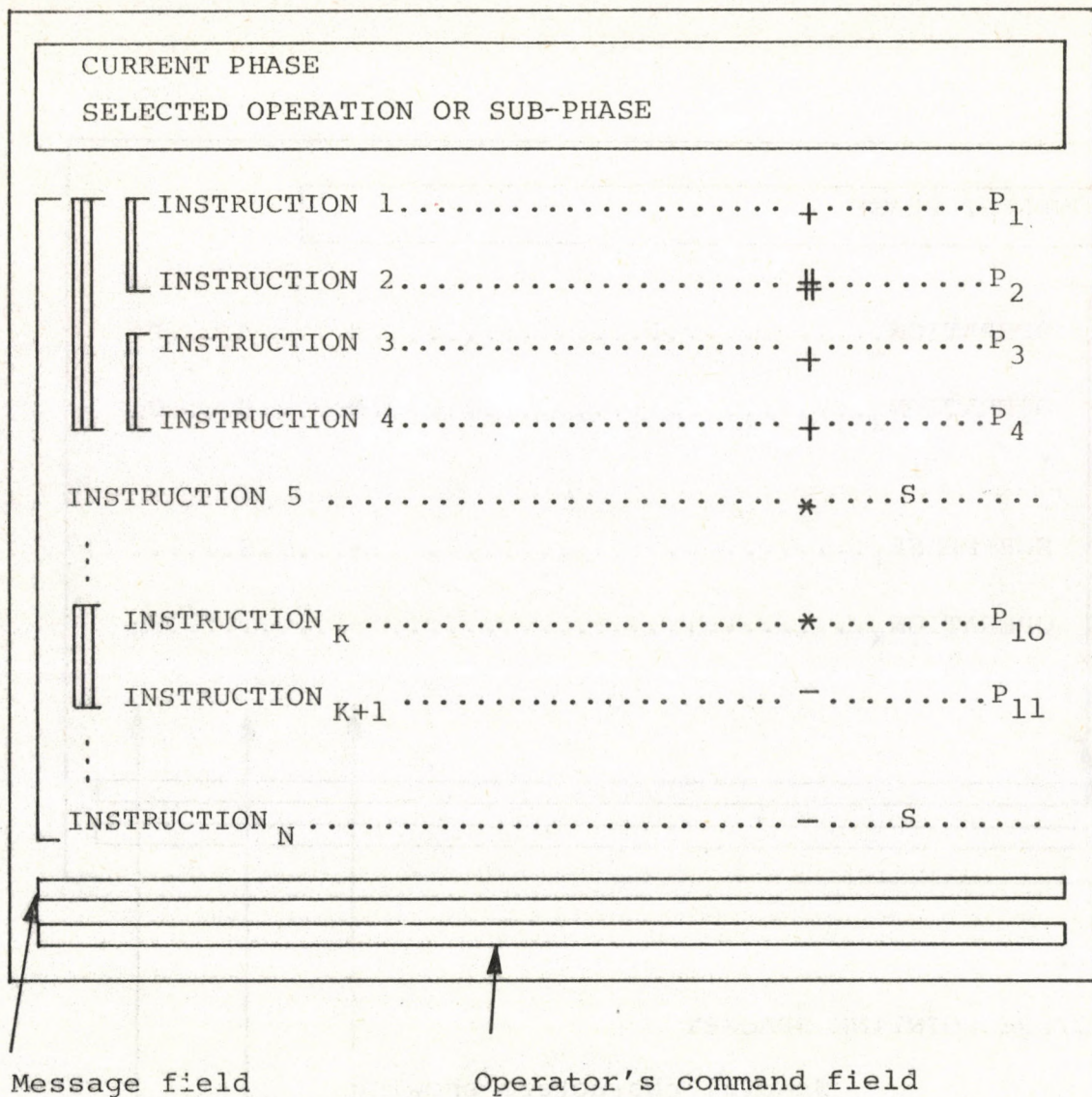


Fig.3. Display format of the instructions on lower levels

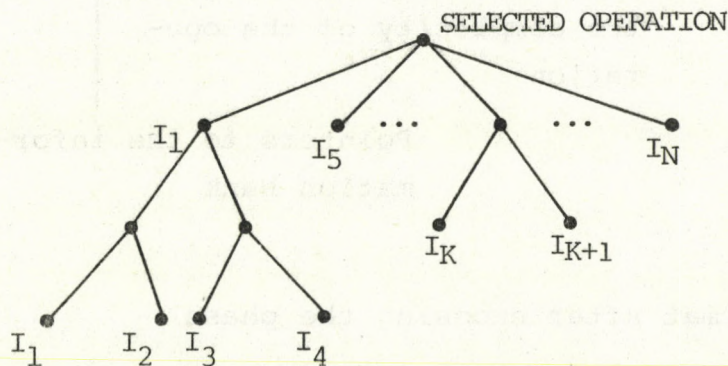


Fig.4. Structure of the displayed format on Fig.3.

has executed it. Then the colour of the given operation or instruction will change. The new colour will show the manipulation mode. After a successful execution the operation will change its colour to "acknowledgement" colour. After having started an operation, it appears in "started" colour. If the operator consciously or by mistake violates the logical operations of the hierarchy, the violated operation will be displayed in "skipped" colour. In this way the operator can observe immediately his mistake. Moreover, in this case the system will send a warning message, too and suspends the operator's activity until the correction of this mistake.

However this suspension concerns only the logical , structural mistakes of the operator and not the real executions.

4. Storage of operations

4.1. Structure of the storage

Not only the great amount of operations, but the data structure reflecting their logical connections have to be stored. The choice of this structure is very important, because it determines how fast and easy will be composed a picture required by the operator.

Let us denote the time sequence and the Boolean algebraic relations as operators. We have introduced the tree structure the nodes of which are $\langle \text{instruction, operator} \rangle$ ordered pairs. The first element of the pair is an instruction reference, the second is the children's operator of the node. Let us introduce the zero instruction and operator as:

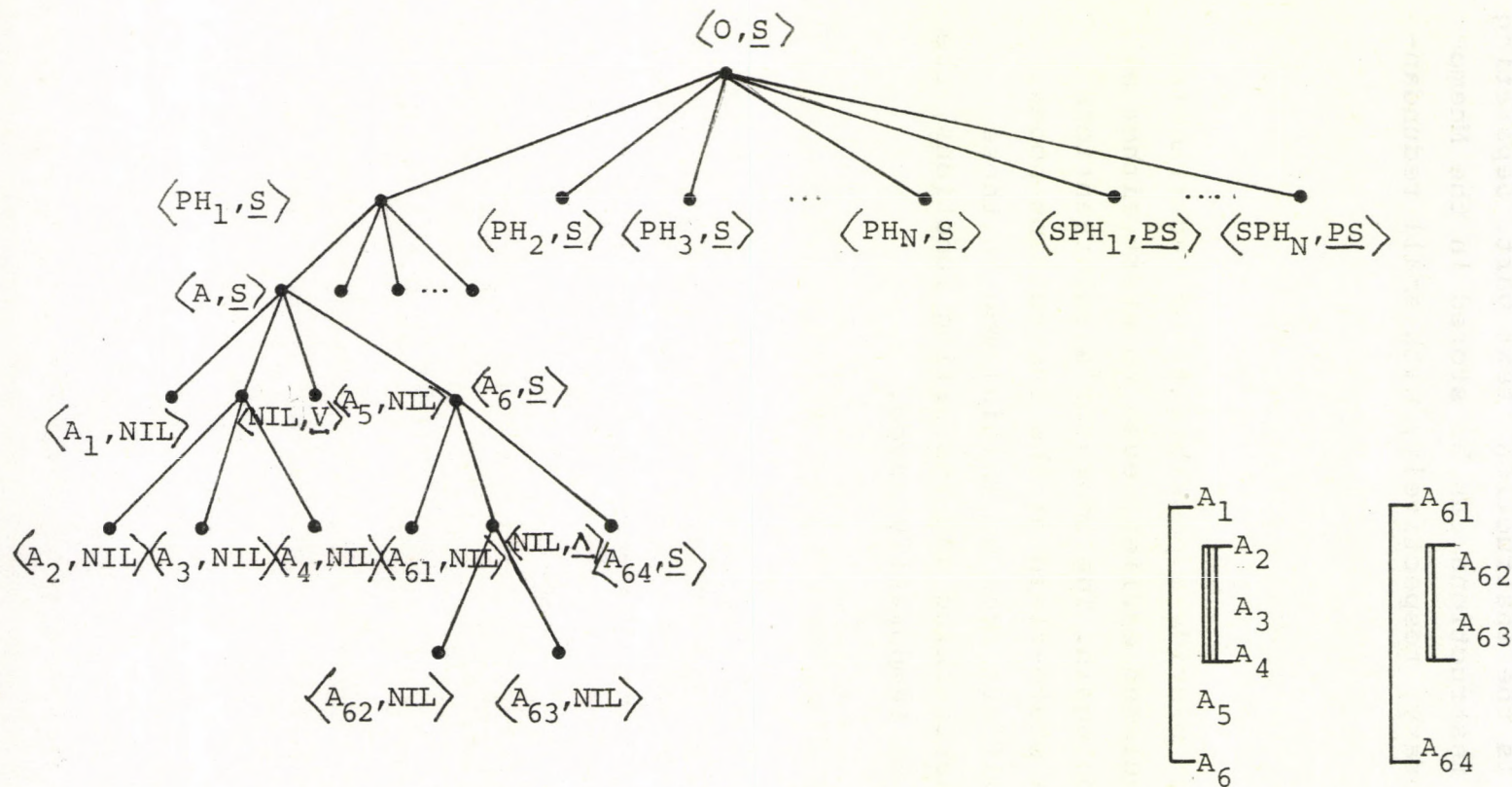
$\langle \text{instruction, NIL} \rangle$: means a simple executable instruction, a terminator

$\langle \text{NIL, operator} \rangle$: this node represents a complex instruction what derives from its children's logical operation.

It is logical to place the sub-phases onto the phase-level because they have the same structure and the redundant storage can be avoided in this way. Fig.5. shows the tree structure.

4.2. Core

The structure describing tree has a great importance during the process but due to its size it is not possible to keep a subtree belonging to a given phase in the operative memory. However the operation level of a tree could be core-resident and could be considered as a bidirectional list.



The operators: \underline{S} : time sequence
 \underline{PS} : time sequence of subphase
 \underline{V} : logical OR connection
 $\underline{\wedge}$: logical AND connection

Fig. 5. The stored tree structure

4.3. Libraries

Every instruction can be divided into two parts: one is the mnemonic, the other is the instruction text part. Separating these two parts the instructions can be stored in the Mnemonic and the Text library, respectively, with small redundancy.

4.4. Saving

The COM system has to provide a possibility of backtracking the operations manipulated earlier, even to start either a phase or an operation again. The operator's interventions are reflected in the state-field of the instruction nodes, i.e. a "used" tree differs from an initial one in these state fields. For backtracking and restarting functions, the used sub-trees must be temporarily saved.

5. The Editor function

The system also offers the possibility to modify easily any parts of the manual via keyboard editing. For the editor function simple and unambiguous identification of the instructions is needed. One of the ways to do it is numbering. In the COM system the numbering is not fixed to the instructions, but it is relative the operation level. Because the organization of communication between data structures shows that the operation list must be core-resident during a phase processing, the operational level is regarded as editor-level. On this level the numbering can be managed easily. Accordingly, here an operation may be inserted or deleted, but it can not be done on lower level. Fig.6. shows how to insert an operation:

Input to the editor:

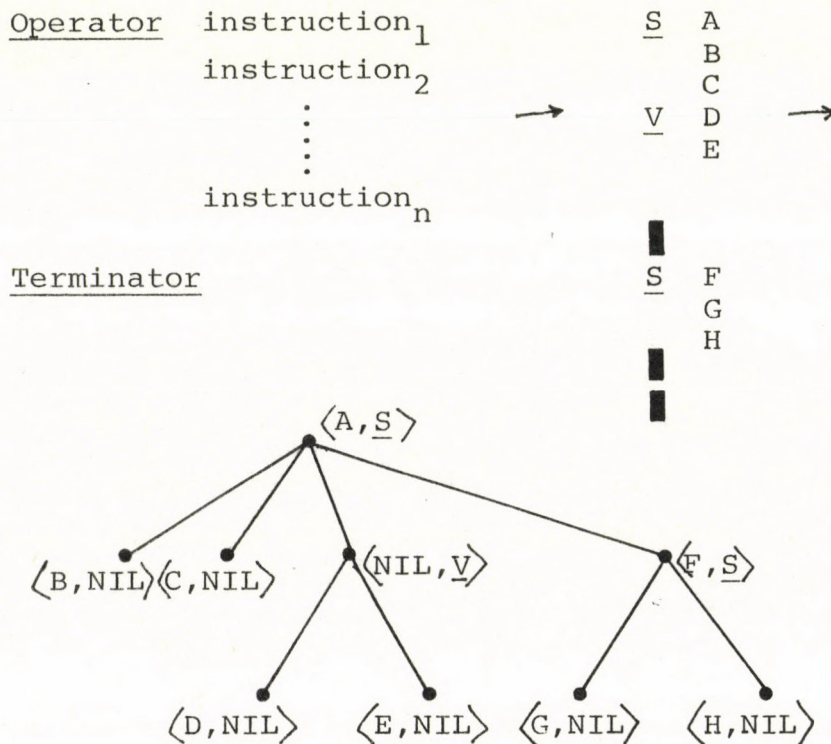


Fig.6. How to insert an operation

6. Hardware resource estimation

The hardware requirement of the COM system of a nuclear power plant has been analysed and it gives the following results:

- number of phases :10-20
- number of operations in
one phase :500-800

With this data, the needed disc capacity is about 6 Mbyte.

References

1. L.P. Goodstein: Procedures for the Operator - their role and support. Proceedings of the IAEA Specialists Meeting. Munich, December, 1979
2. A. Nedelik, H. Roggenbauer: A Computerized System for Evaluation of the Status of a Protection System. Proceedings of IAEA Specialists' Meeting. Munich, December 1979
3. A Computer-based System to Aid the Operator to Survey the Status of Reactor Safety System in BWR's. OECD Halden Reactor Project Report. December, 1979
4. F. Dworzak, A. Nedelik, P. van Gernst: Design and Implementation of a Computerized System for Evaluation of Plant Status with Respect to Safety Technical Regulations. Proceedings of the IAEA International Symposium, Munich, October, 1982.
5. H. Roggenbauer: Methods and Techniques used in Computerized Operator Support System for German NPPs. Proceedings of the IAEA Specialists' Meeting. Balatonaliga, October 1983
6. C.H. Meijer, W.J. Gill: Operational Aids to Improve the Man-Machine Interaction in a Nuclear Power Plant. Proceedings of the Annual Meeting of the American Nuclear Society Las Vegas. June, 1980

7. W.R. Corcoran and others: The Operator's Role and Safety Functions. Proceedings of the Workshop on Licensing and Technical Issues - post TMI. Washington, March, 1980.
8. H. Joshitoshi and others: Development of Computerized Operator Support System. Proceedings of The IAEA International Symposium. Munich, October, 1982.
9. P. Fazekas: Proposal of setting in hierarchical order the operational instructions, March, 1983



Kiadja a Központi Fizikai Kutató Intézet
Felelős kiadó: Gyimesi Zoltán
Szakmai lektor: Végh Endre
Nyelvi lektor: Végh Endre
Példányszám: 155 Törzsszám: 84-361
Készült a KFKI sokszorosító üzemében
Felelős vezető: Nagy Károly
Budapest, 1984. május hó